DETAILED ACTION

1. Applicant's amendment filed on May 21, 2008 has been entered. Claims 6-8 are pending. Claims 1-5 and 9-11 are cancelled by the applicant.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given by applicant's amendment filed on June 4, 2008. The applicant has agreed to authorize examiner to incorporate the entire limitations of claim 7 into claim 6 and to cancel claim 7.

CLAIMS:

3. Please cancel claim 7.

Please replace claim 6 as follow:

6. A method of detecting privilege escalation vulnerabilities in a pre-existing source code listing, said source code listing having a listed sequence of expressions, each expression including a set of operands and operators to transform values of the operands, said source code listing further having routine calls, said routine calls including arguments with which to invoke a routine, said source code listing being stored in computer readable medium having computer executable instructions, wherein a privilege escalation vulnerability is an uncontrolled escalation of system privileges that allows unauthorized access to system resources, the method comprising:

providing a list specifying routines that potentially cause privilege escalation vulnerabilities;

providing pre-specified ranges of values for arguments of routines in the list that cause privilege escalation vulnerabilities;

analyzing the source code listing to identify calls to routines specified in the list;

analyzing the source code listing to semantically analyze arguments of the identified routine calls to determine routine calls that possess privilege escalation vulnerabilities using the pre-specified ranges of values;

wherein semantically analyzing the arguments of the identified routine calls comprises analyzing the source code listing to create computer models of the arguments, each model specifying a range of values that each corresponding argument can take when the source code listing is executed; and

generating a report that identifies the vulnerabilities.

Information Disclosure Statement

4. The information disclosure statement (IDS) filed on February 21, 2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Allowable Subject Matter

5. Claims 6 and 8 are allowed. The following is an examiner's statement of reasons for allowance: The prior art does not disclose a method of detecting privilege escalation vulnerabilities in a pre-existing source code listing, said source code listing having a listed sequence of expressions, each expression including a set of operands and operators to transform values of the operands, said source code listing further having routine calls, said routine calls including arguments with which to invoke a routine, said source code listing being stored in computer readable medium having computer executable instructions, wherein a privilege escalation vulnerability is an uncontrolled escalation of system privileges that allows unauthorized access to system resources, the method comprising: providing a list specifying routines that potentially cause privilege escalation vulnerabilities; providing pre-specified ranges of values for arguments of routines in the list that cause privilege escalation vulnerabilities; analyzing the source code listing to identify calls to routines specified in the list; analyzing the

source code listing to semantically analyze arguments of the identified routine calls to determine routine calls that possess privilege escalation vulnerabilities using the pre-specified ranges of values; wherein semantically analyzing the arguments of the identified routine calls comprises analyzing the source code listing to create computer models of the arguments, each model specifying a range of values that each corresponding argument can take when the source code listing is executed; and generating a report that identifies the vulnerabilities as set forth in claim 6.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

TBT
June 4, 2008